TAMPEREEN
AMMATTIKORKEAKOULU

Palvelin Tor-verkossa

Sampsa Johannes Lehtonen

Opinnäytetyö
Huhtikuu 2016
Tietojenkäsittely
Tietoverkkopalvelut

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely
Tietoverkkopalvelut

LEHTONEN, SAMPSA JOHANNES:
Palvelin Tor-verkossa

Opinnäytetyö 34 sivua
Huhtikuu 2016

Tor on internetliikenteen suojaamiseen tarkoitettu ohjelmisto. Tor-verkon tarkoituksena on piilottaa ja suojata internetliikenne niin, että sitä ei voida seurata. Tässä opinnäytetyössä asennettiin palvelin, jonka tarkoituksena oli hyödyntää Tor-verkkoa. Tavoitteena oli tutkia, kuinka Tor-verkossa voidaan hallinnoida palvelinta anonyymisti. Menetelmänä käytettiin kvalitatiivista tapaustutkimusta, jossa palvelimelle asennettiin kaksi palvelua, jotka olivat saavutettavissa vain Tor-verkon kautta.

Palvelinlaitteistona käytettiin Raspberry Pi -tietokonetta. Tälle palvelinlaitteistolle asennettiin web-palvelinohjelmisto Nginx, Simple Machines Forum -keskustelupalstaohjelmisto, sekä Tor-ohjelmisto. Toinen palveluista oli web-sivu, joka julkaistiin osoitteessa http://xlclklszcjk5ry5t.onion, ja toinen keskustelupalsta, joka julkaistiin osoitteessa http://3x3pgkebmo6hdm32.onion. Nämä kaksi palvelua olivat tavoitettavissa vain Tor-verkon kautta eikä niiden sijaintia voida saada selville.

Palveluiden asettaminen toimintaan Tor-verkkoon oli yksinkertaista. Ero palveluiden julkaisemisessa Tor-verkossa ja julkiverkossa on hyvin pieni. Ohjelmista käytettiin uusimpia versioita, joita paketinhallinnasta oli saatavilla. Paketinhallinnassa ei aina ole ohjelmien uusimpia versioita, niinpä joitain tietoturva-aukkoja saattaa käytetyistä ohjelmista löytyä, jotka voivat paljastaa palvelimen sijainnin.

Asiasanat: tor, palvelin, tietoturva, yksityisyys

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems
Option of Network Services

LEHTONEN, SAMPSA JOHANNES:
A Server on the Tor Network

Bachelor's thesis 34 pages
April 2016

The objective of this study was to gather information on how to anonymously host a server on the Tor network. The purpose of on hosting servers on Tor is to hide the location of the server.

This study was carried out as a project where the web-server program Nginx and forum tool Simple Machines Forum were installed on a device. These two were then configured to be accessible from Tor. Both tools are open source and free software. The device used was Raspberry Pi, a low-cost piece of hardware. The operating system chosen to be installed on this hardware was Minibian, which is a derivative of the Linux Debian operating system.

As a result, two services were hosted on the Tor network. Access to these services was done with a browser that can connect to Tor. The services did not provide information where the server was located.

Further work is needed to secure the service hosting. The software's used here are not the newest versions so far released. To get the newest software possible, it must be built directly from the source. Newer software has security updates that will fix issues that might compromise location of the server.

Key words: tor, server, security, privacy

SISÄLLYS

1 JOHDANTO

Yksityisyydellä on monia eri merkityksiä. Laajasti käsiteltynä se voidaan ymmärtää tarkoittavan oikeutta jätettäväksi rauhaan tai oikeutta suojautua ulkopuolisesta puuttumiselta. Yksityisyys on Suomen perustuslaissa turvattu oikeus. Internetissä yksityisyys voidaan käsittää sisältävän henkilön tunnistamiseen riittävät tiedot, kuten ikä ja osoite ja tiedot, joiden perusteella käyttäjä voidaan tunnistaa, kuten käyttäytyminen internetsivustolla. Monet internetpalvelut keräävät näitä tietoja, sillä sen avulla voidaan tarjota käyttäjille esimerkiksi kohdennettua mainontaa. On kuitenkin tapoja, joilla käyttäjät voivat piilottaa tiedot, joista näiden henkilöllisyys saataisiin selville. Yksi tapa on käyttää Tor-verkkoa. Tor-verkon avulla voidaan salata internetliikenne niin, että käyttäjän tai kohdepalvelimen sijainti ei ole tiedossa.

Tässä opinnäytetyössä asennetaan palvelin, joka käyttää hyödykseen Tor-verkkoa. Tor-verkon avulla palvelimen hallinnoija voi piilottaa palvelimen sijainnin niin, että sitä ei ole mahdollista paikantaa. Piilottamalla palvelin voidaan saada palvelimen hallinnoijalle mahdollisimman suuri anonymiteetti ja yksityisyydensuoja. Tor-verkossa olevat palvelimet ovat selattavissa vain erityisellä selaimella, joka on konfiguroitu toimimaan Tor-verkossa.

Opinnäytetyön tavoitteena on saada tietoa siitä, kuinka palvelimia pystytään hallinnoimaan täysin anonyymisti ja tietoturvallisesti internetissä. Tarkoituksena on asentaa palvelin, joka hyödyntää Tor-verkkoa palvelimen liikennöinnissä. Palvelinohjelmisto asennetaan vähän virtaa kuluttavalle Raspberry Pi 2 -tietokoneelle. Kun palvelin on oikein asennettu ja konfiguroitu, voidaan palvelimelle päästä vain Tor-verkon avulla. Opinnäytetyö on onnistunut, kun palvelin on asennettu toimimaan Tor-verkossa niin, että sen sijaintia ei voida selvittää.

2 TOR

Tor on avoimen lähdekoodin ohjelmisto, joka on kehitetty salaamaan tietoliikenne. Se mahdollistaa anonymiteetin internetin käytön ja sensuurin kiertämisen. Tor myös pystyy piilottamaan käyttäjän oikean sijainnin. Tor-verkko koostuu palvelimista ja reitittimistä, joihin on asennettu Tor-ohjelmisto. Tämä verkko on usean, yli seitsemästä tuhannesta solmusta koostuva maksuton, maailmanlaajuinen ja vapaaehtoistyöllä ylläpidettävä verkosto (Tor Network Status, 2016). Käyttäjä voi Tor-verkon avulla suojata yksityisyytensä sekä suojata itsensä valvontaa ja seurantaa suorittavilta tahoilta.

Tor-verkon toimintaperiaate perustuu liikkuvan datan salaamiseen ja kierrättämiseen usean eri Tor-reitittimen kautta. Data kierrätetään kolmen eri Tor-reitittimen kautta ennen kuin liikenne menee kohdepalvelimelle. Tätä tekniikkaa käyttäessä kohdepalvelin ei voi tietää, mistä liikenne oikeasti tulee, sillä se näkee vain sitä edeltävän palvelimen.

2.1 Historia

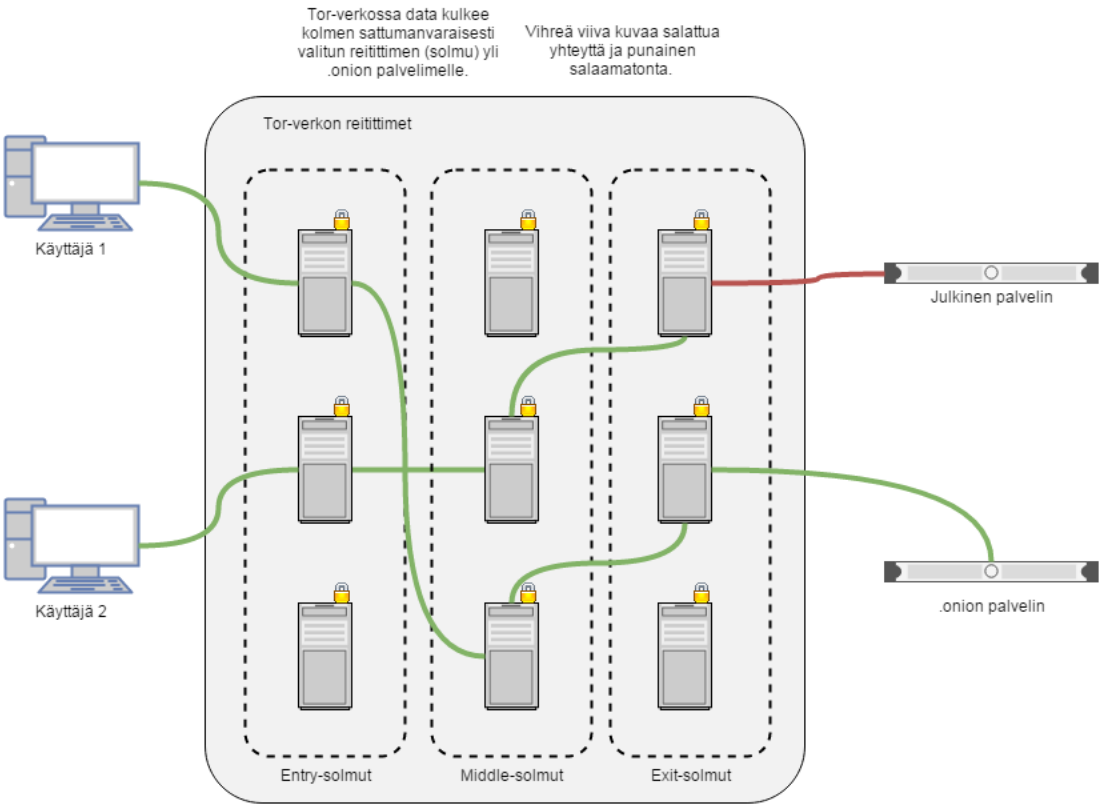
Tor-ohjelmisto on alun perin Yhdysvaltojen laivaston tutkimuslaitoksen kehittämä. Alkuperäinen nimi on TOR, joka tulee sanoista The Onion Router. Tor-verkon alfaversio julkaistiin syyskuussa 2002. Vuonna 2004 hanke julkaistiin vapaan lisenssin alla, jolloin Electronic Frontier Foundation (EFF) rahoitti projektin kehittämisen edistämiseksi. Joulukuussa 2006 perustettiin järjestö The Tor Project, joka otti haltuun Tor-verkon kehittämisen. Tor Projectin rahoittajiin kuuluu nykyään yksityishenkilöitä, verkkosivusto Reddit, Yhdysvaltojen valtion virasto sekä monia muita tahoja.

2.2 Tor-verkon toiminta

Tor-verkko koostuu kolmesta erilaisesta Tor-reitittimestä, niin kutsutuista solmuista (kuva 1). Näitä reitittimiä ovat entry-solmu, middle-solmu ja exit-solmu (Wright, How Tor Works? 2015). Entry-solmun tehtävä on vastaanottaa ensimmäinen yhteys käyttäjältä. Tämä on ensimmäinen askel Tor-verkossa. Middle-solmun tehtävä on ottaa vastaan liikenne entry-solmulta ja viedä se exit-solmulle. Exit-solmun tehtävä on lähettää ja vastaanottaa liikenne julkiseen verkkoon. Julkisessa verkossa oleva palvelin näkee liikenteen tulevan exit-solmulta eikä käyttäjältä itseltään. Toiminta on hieman erilainen, jos kohdepalvelin sijaitsee Tor-verkossa. Tällöin liikenne ei mene exit-solmulle, vaan toiselle middle-solmulle, joka toimii linkkinä piilopalvelimelle.

Liikenne Tor-reitittimien välillä kulkee salattuna. Ensiksi käyttäjän liikenne salataan niin, että vain exit-solmu pystyy avaamaan salauksen. Tämä salattu liikenne salataan uudestaan niin, että middle-solmu pystyy avaamaan salauksen. Viimeiseksi kahdesti salattu liikenne salataan kolmannen kerran niin, että entry-solmu pystyy avaamaan salauksen. Näin tehtäessä jokaisella solmulla on sellaista tietoa, mitä se tarvitsee, eli mistä salattu liikenne on tullut ja mihin lähettää se seuraavaksi.

Tor-verkon solmukohdat ovat julkista tietoa. Koska tämä tieto on julkista, voi sensuuria harjoittava taho estää pääsyn näihin solmukohtiin. Esimerkiksi, jos pääsy entry-solmuihin estetään, ei pääsyä Tor-verkkoon ole. Siksi on myös kehitetty niin kutsuttu bridge-solmu. Bridge-solmu on toimintaperiaatteeltaan samanlainen kuin entry-solmu, mutta tietoa mitkä palvelimet toimivat bridge-solmuina, ei ole julkisesti saatavilla.



KUVA 1. Tor-verkon toimintaperiaate

2.3 Miksi käyttää Tor-verkkoa?

Tor-verkkoa voidaan hyödyntää muun muassa tilanteissa, joissa tiedon paljastaminen tai esilletuonti voi asettaa tiedon paljastajan vaaraan. Esimerkkinä voi olla vaikka tilanne, jossa henkilö saa tietoa väärinkäytöksistä valtion johdossa, mutta ei voi tuoda sitä esille,

koska pelkää johdossa olevien henkilöiden kostoa. Tämä henkilö voi saattaa julkiseksi tämän tiedon Tor-verkon avulla paljastamatta omaa henkilöllisyyttään.

Vuonna 2013 Edward Snowden vuoti journalistien välityksellä julkisuuteen Yhdysvaltojen tiedustelupalvelu NSA:n harjoittaman yksityishenkilöitä ja yrityksiä kohtaan kohdistetun massavakoilun. Hän hyödynsi Tor-verkkoa pitäessään yhteyttä journalistien kanssa.

Tor-verkon avulla myös maissa, joissa harjoitetaan sensuuria, saavat sen maan asukkaat mahdollisuuden selata sivustoja, jotka on joko sensuroitu kokonaan tai osittain. Eräs paljon sensuuria harjoittava maa on Kiina. Kuvassa 2 on kuvankaappaus greatfirewallofchina.org -sivustolta. Tämän sivuston avulla voidaan kokeilla, onko jokin sivusto sensuroitu Kiinassa. Kuten kuvasta 2 ilmenee, osoitteeseen www.youtube.com ei ole pääsyä. Internetin käyttäjät Kiinassa voivat selata YouTubea Tor-verkon kautta.

KUVA 2. kuvankaappaus greatfirewallofchina.org -sivustolta

2.4 Tor-verkon heikkouksia

Tor-verkko on hyvä tapa suojata liikenne urkinnalta ja häirinnältä, mutta sekään ei ole täydellinen. On tapoja, joilla käyttäjä voidaan tunnistaa ja liikennettä seurata. Tor-verkon

toimintaan ei kuulu koko liikenteen suojaaminen. Jos Tor-verkon kautta selataan julkisessa internetissä olevaa http-palvelinta, liikenne exit-solmun ja julkisen palvelimen välillä ei kulje salattuna, koska http-protokolla ei ole salattua. Tällöin on mahdollista, että exit-solmun ylläpitäjä pystyy seuraamaan, mitä tietoa palvelimien välillä kulkee.

Jotkut protokollat voivat paljastaa käyttäjän IP-osoitteen. Esimerkiksi BitTorrent protokolla voi paljastaa käyttäjän IP-osoitteen. Monet torrent-ohjelmat käyttävät hyödykseen niin sanottua DHT-protokollaa, joka myös saattaa paljastaa käyttäjän IP-osoitteen. BitTorrent protokollaa ei suositella käytettävän Tor-verkossa, sillä se lisää verkon liikennettä, mikä sen myötä hidastaa koko Tor-verkkoa (The Tor Project, Bittorrent over Tor isn't a good idea 2010).

Tor-verkkoa suositellaan käyttämään Tor Browserilla. Tor Browser on muokkaus Firefox-selaimesta, joka on valmiiksi konfiguroitu toimimaan Tor-verkossa. Mahdolliset haavoitukset Firefox-selaimessa voivat paljastaa käyttäjien sijainnin.

3 TIETOTURVA

Tietoturva on digitaalisen tiedon, palvelujen, järjestelmien ja tietoliikenteen suojaaminen ulkopuolisilta. Tietoturvauhkia ovat luvaton pääsy, tiedon luvaton käyttö, salaisen tiedon paljastuminen, tiedon sekaannus, tiedon muuntuminen, salaisen tiedon tutkituksi tuleminen, tiedon kopioituminen ja tiedon hävittäminen. Tietoturvan suojausmenetelmät voidaan jakaa kolmeen eri ryhmään: tekniseen, fyysiseen ja hallinnolliseen (Suomen Internetopas, Suojausmenetelmät).

3.1 Tekninen tietoturva

Tekninen tietoturva tarkoittaa, että käytetään laitteistoa ja ohjelmistoa, jossa ei ole tietoturvapuutteita. Täydellistä teknistä tietoturvaa olevaa ohjelmaa ei ole olemassakaan, joten on tärkeää päivittää käytetyt laitteet ja ohjelmistot. Päivitykset korjaavat tietoturva-aukkoja, joiden avulla hyökkääjä voi mahdollisesti saada palvelimen kokonaan hallintaansa tai kerätä tietoja ylläpitäjästä tai palvelimella olevasta tiedosta.

Tekniseen tietoturvaan kuuluu myös salauksen, vahvojen salasanojen, kaksivaiheinen tunnistautumisen käyttö, anti-virus ja palomuurin käyttö. Salauksessa data salataan niin, että se ei ole luettavissa vaikka joku datan saisikin haltuun. Vahvat salasanat tekevät salasanojen veikkaamisesta hankalaa. Brute-force-hyökkäyksessa salasanaa arvataan koneellisesti, jopa satoja miljardeja eri yhdistelmiä sekunnissa (Goodin 2012). Vahva salasana tekee brute-force-hyökkäämisestä niin aikaa vievää ja kallista, että sitä ei voida murtaa. Kaksivaiheisella tunnistautumisella varmennetaan henkilön identiteetti kahdella eri menetelmällä. Esimerkiksi kirjautuminen sähköpostiin voidaan todentaa kahdella menetelmällä. Ensimmäinen on käyttäjätunnus ja salasana -yhdistelmä ja toinen on matkapuhelimeen lähetettävä tekstiviesti. Jos tunkeutuja saa haltuunsa käyttäjätunnuksen ja salasanan, ei hänellä silti ole pääsyä henkilön sähköpostiin. Palomuurin tehtävä on estää haluamaton liikenne verkossa. Sen avulla voidaan esimerkiksi estää liikenne tiettyihin portteihin, kuten porttiin 22, joka on SSH:n käyttämä portti. Anti-viruksen tehtävä on suojata kohdekonetta viruksilta, jotka voivat tarttua internetin kautta ladatuista tiedostoista tai haitallisista sivustoista.

3.2 Fyysinen tietoturva

Fyysinen tietoturva tarkoittaa laitteiston, henkilöstön, ohjelmiston, tietoverkkojen ja datan suojaamista. Fyysiseen tietoturvaan kuuluu suojaamista tulipalolta, varkauksilta,

luonnon katastrofeilta ja vandalismilta. Laitteistoa voi suojata asettamalle ne paikkaan, johon harvoilla on pääsy, kuten lukittuun palvelinhuoneeseen. Lukitun palvelintilan tarkoituksena on estää pääsy henkilöiltä, jotka yrittävät varastaa tietoa tai laitteistoa. Se myös suojaa vahingoilta, joita tietämätön henkilö voi vahingossa saada aikaan. Tämä tila voidaan myös suojata tulipaloilta asettamalla automaattiset sammuttimet. Valvonta ja automaattiset hälytykset auttavat turvaamaan suojatulle alueelle tunkeilijoilta.

3.3 Hallinnollinen tietoturva

Hallinnollisella tietoturvalla tarkoitetaan henkilöiden tietoturvaosaamista. Käytännössä se on eri tietoturvauhkien ymmärtämistä sekä niitä toimia, joilla näitä uhkia voidaan pienentää tai estää. Yrityksissä hallinnollista tietoturvaa voidaan parantaa ohjeistamalla ja kouluttamalla työntekijöitä. Työntekijöiden tulee esimerkiksi ymmärtää salasanojen oikeaoppinen käyttäminen. Salasanoja ei saa kirjoittaa lapuille, eikä sitä saa kenellekään muulle kertoa ja sen on oltava riittävän pitkä ja monimutkainen. Hallinnolliseen tietoturvaan kuuluu myös dokumentit, kuten tietoturvapolitiikka, sekä vastuualueiden jakaminen. Yrityksen on tiedettävä, mitä toimenpiteitä pitää tehdä, jos jokin tietoturvauhka tapahtuu. Uhkien tiedostaminen ja niihin varautuminen vähentää aikaa, jota kuluu yritystoiminnan palautuessa tietoturvauhasta.

4 TOTEUTUS

Opinnäytetyössä asennetaan Minibian-käyttöjärjestelmä Raspberry Pi 2 -laitteistolle. Minibian perustuu Debian-käyttöjärjestelmään. Tälle palvelimelle asennetaan web-palvelinohjelmisto Nginx, joka liitetään Tor-verkkoon. Ngnixn avulla Tor-verkossa julkistetaan kaksi palvelua: yksi staattinen web-sivusto sekä keskustelupalsta. Asetusten jälkeen näihin palveluihin ei ole pääsyä julkisen verkon kautta.

4.1 Käyttöjärjestelmän asennus

Minibian-käyttöjärjestelmän latauksessa ja asennuksessa käytetään seuraavaa järjestystä:

1. Ladataan käyttöjärjestelmä.
2. Asennetaan ladattu käyttöjärjestelmä Micro SD -kortille.
3. Laajennetaan koko Micro SD -kortti käyttöjärjestelmän käyttöön.

Käyttöjärjestelmä ladataan ohjelman projektisivulta, joka on http://sourceforge.net/projects/minibian/files/. Tarkistetaan ladatun tiedoston SHA1 -tunniste, jotta varmistutaan, että ladattu tiedosto ei ole korruptoitunut. Tunnusta verrataan Minibian-projektisivulla annettuun tunnisteeseen:

```
sha1sum 2015-02-18-wheezy-minibian.tar.gz
```

Seuraavaksi Minibian asennetaan Micro SD -kortille hakemistoon /dev/sdd komennolla:

```
sudo dd bs=4M if=2015-02-18-wheezy-minibian.img of=/dev/sdd
```

IP-osoite (Internetin protokollaosoite) yksilöi laitteen käyttämän osoitteen ja DHCP-palvelimen (Dynamic Host Configuration Protocol) tehtävä on jakaa IP-osoitteita lähiverkkoon kytkeytyville laitteille. Raspberry Pi saa IP-osoitteen 192.168.0.102 automaattisesti DHCP-palvelimelta.

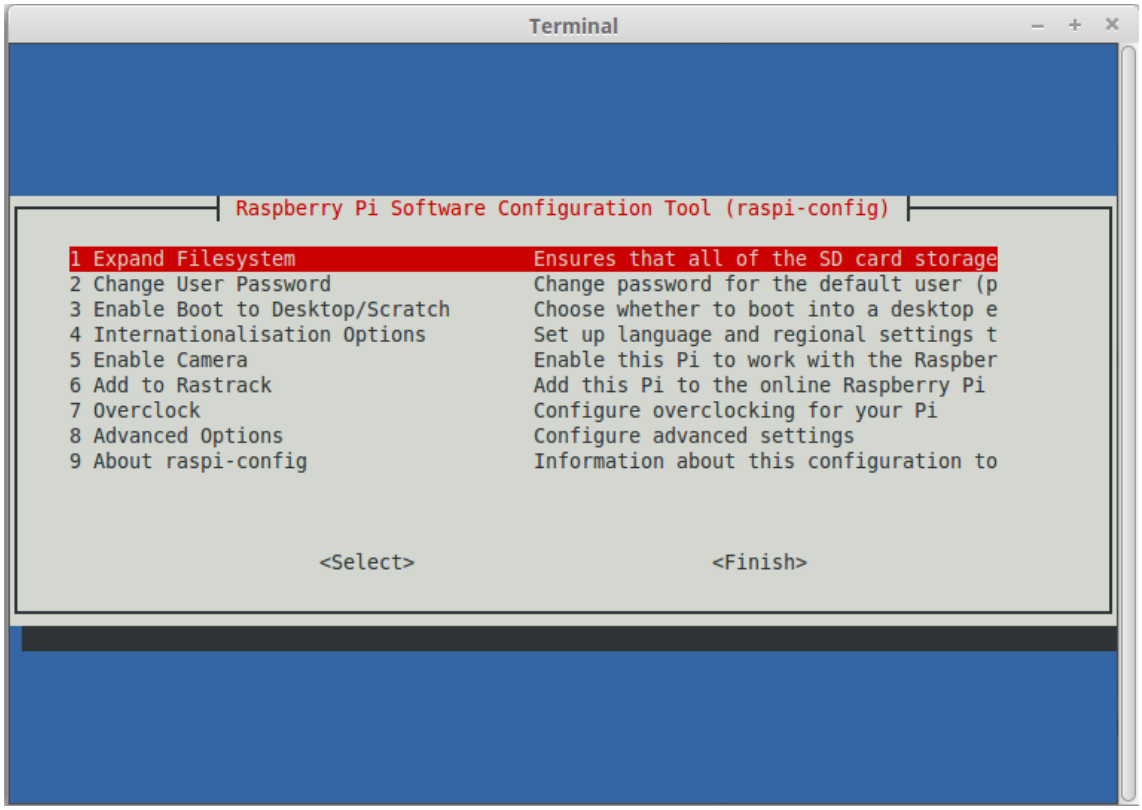
Palvelimelle kirjaudutaan käyttämällä oletuskäyttäjätunnusta ja salasanaa, jotka ovat *root* ja *raspberry*. Ensimmäisen kirjautumisen jälkeen laajennetaan palvelin käyttämään koko Micro SD -kortin vapaata tilaa, jotta kaikki saatavilla olevat päivitykset voidaan asentaa. Tämä tehtiin käyttämällä raspi-config-ohjelmaa, joka pitää ensin asentaa komennolla:

apt-get install raspi-config –y

Ohjelma käynnistetään komennolla:

raspi-config

Valikosta valitaan ensimmäinen kohta, Expand Filesystem (kuva 3). Komento automaattisesti laajentaa kaiken vapaan tilan palvelimen käyttöön. Nämä muutokset tulevat voimaan uudelleen käynnistyksen yhteydessä.



KUVA 3. raspi-config valikko

Tämän jälkeen päivitetään käyttöjärjestelmä. Koska Minibianin viimeisin asennustiedosto on luotu 18. helmikuuta 2015, päivitys ensimmäisellä kerralla kestää jonkin aikaa.

apt-get update && apt-get upgrade –y

Jotta kaikki päivitykset tulevat käyttöön, palvelin käynnistetään uudestaan komennolla:

```
shutdown -r now
```

Minibian-käyttöjärjestelmä ja päivitykset ovat nyt asennettu. Seuraavassa osiossa muokataan käyttöjärjestelmän asetuksia.

4.2 Käyttöjärjestelmän konfigurointi

Käyttöjärjestelmän asetuksien muokkaamisessa käytetään seuraavaa järjestystä:

1. Asetetaan staattinen IP-osoite.
2. Lisätään uusi käyttäjätunnus.
3. Luodaan SSH-avain.
4. Estetään palvelimelle kirjautuminen ilman SSH-avainta.

Palvelimella on käytössä DHCP-palvelimelta saatu IP-osoite 192.168.0.102. DHCP-palvelimelta saatu IP-osoite voi muuttua, joten vaihdetaan palvelimen IP-osoite muuttumattomaksi, staattiseksi. Staattinen IP-osoite varmistaa, että palvelimen IP-osoite pysyy aina samana. Tämä tehdään muokkaamalla */etc/network/interfaces* tiedostoa:

```
vim /etc/network/interfaces
```

Tiedosto muokataan käyttämään 192.168.0.50 IP-osoitetta. Kohdassa *iface eth0 intet static* kerrotaan palvelimen käyttävän staattista IP-osoitetta. IP-osoite annetaan kohtaan *address*, aliverkon peite kohtaan *netmask* ja palvelimen käyttämä yhdyskäytävä *gateway* kohtaan. Tiedoston asetukset ovat:

```
auto eth0
iface eth0 inet static
    address 192.168.0.50
    netmask 255.255.255.0
    gateway 192.168.0.254
```

Jotta asetukset tulevat voimaan, käynnistetään palvelimen verkko uudelleen. Tämä komento katkaisee yhteyden palvelimeen. Uusi yhteys aukaistaan vaihdettuun IP-osoitteeseen.

service networking restart

Root-käyttäjätunnusta on käytetty palvelimelle kirjautumisessa. Root-käyttäjätunnus otetaan kokonaan pois käytöstä, mutta ennen sitä luodaan uusi käyttäjätunnus, jolla kuitenkin on riittävät oikeudet muokata järjestelmäasetuksia. Palvelimelle lisätään käyttäjätunnus *tor*. Se luodaan komennolla:

adduser tor

Tälle käyttäjälle annetaan oikeudet muokata järjestelmäasetuksia komennolla:

adduser tor sudo.

Tästä lähtien palvelimeen otetaan yhteys tor -käyttäjätunnuksella. Seuraavaksi luodaan SSH-avainpari. SSH-avaimia on kaksi kappaletta, toinen on julkinen avain ja toinen yksityinen. Julkinen avain säilyy palvelimella ja yksityinen avain on etäyhteyskoneella. On erittäin tärkeää pitää yksityinen avain hyvin suojattuna, sillä avain on pääsy palvelimelle. Avainta luodessa siihen on suositeltavaa lisätä avainfraasi, joka estää avaimen käytön suoraan ilman minkäänlaista salasanaa.

SSH-avainpari luodaan komennolla:

ssh-keygen

Komento pyytää määrittämään, mihin ja millä nimellä avaimet luodaan. Komento pyytää myös antamaan avainfraasin, joka on kuin salasana SSH-avainparille. SSH-avaimet on luotu, joten siirretään julkinen avain palvelimelle. Avain on mahdollista siirtää komennolla *ssh-copy-id –i <tiedoston sijainti> käyttäjätunnus@palvelin.*

ssh-copy-id -i ~/.ssh/id_rsa.pub tor@192.168.0.50

Kun kirjautuminen onnistuu SSH-avaimella, estetään kirjautuminen palvelimelle ilman SSH-avainta. Samalla estetään root-käyttäjällä kirjautuminen. Muokataan sshd_config tiedostosta kolmea asetusta. *PasswordAuthentication no* estää kirjautumisen käyttämällä

vain salasanaa, kuten myös *ChallengeResponseAuthentication no* -asetus. *PermitRootLogin no* -asetus estää kirjautumisen root-käyttäjätunnuksella.

PasswordAuthentication no
ChallengeResponseAuthentication no
PermitRootLogin no

Muokatut asetukset tulevat käyttöön kun SSH-ohjelmisto käynnistetään uudestaan. SSH voidaan uudelleen käynnistää komennolla *sudo service ssh reload*:

sudo service ssh reload

Voidaan varmistaa, että kirjautuminen ilman SSH-avainta on estetty kokeilemalla kirjautua root-käyttäjätunnuksella. Kirjautuminen vain salasanan avulla on estetty, kun kirjautuessa tulee ilmoitus *Permission denied (publickey)*:

ssh root@192.168.0.50
Permission denied (publickey).

4.3 Tor-ohjelmiston asennus

Tor-ohjelmiston asennuksessa ja asetusten asettamisessa käytetään seuraavaa järjestystä:

1. Ladataan ja asennetaan Tor-ohjelmisto
2. Muokataan torrc-tiedostosta asetuksia
3. Tarkistetaan Tor-ohjelmiston luoma Tor-verkon linkki

Tor-ohjelmisto on paketinhallinnasta ladattavissa, josta se ladataan ja asennetaan komennolla:

sudo apt-get install tor

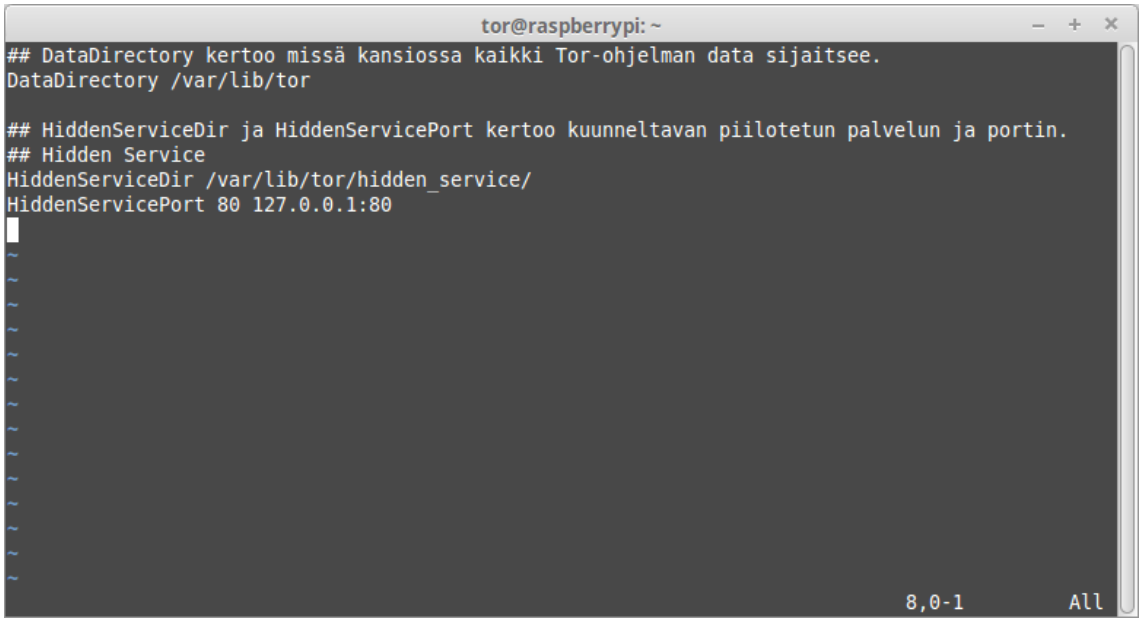
Tor-ohjelmiston asetuksia muokataan /etc/tor/*torrc* -tiedostoon. Asennettaessa Tor loi tiedoston, jossa on listattuna kaikki mahdolliset asetusvalinnat. Tämä tiedosto kopioidaan ja

lisätään tyhjä asetustiedosto, jolloin tiedoston luettavuus on selvempi. Alkuperäinen tiedosto muokataan komennolla *sudo mv /etc/tor/torrc /etc/tor/torrc.bak*. Uusi tyhjä asetustiedosto luodaan komennolla *sudo touch /etc/tor/torrc*.

```
sudo mv /etc/tor/torrc /etc/tor/torrc.bak
sudo touch /etc/tor/torrc
```

Tyhjään torrc-tiedostoon lisätään tiedot, jota Tor käyttää hyödykseen (kuva 4). *DataDirectory* asetus kertoo, missä kansiossa kaikki Tor-ohjelmiston data sijaitsee. *HiddenServiceDir* ja *HiddenServicePort* kertoo kuunneltavan piilotetun palvelun kansion ja käytetyn portin.

```
DataDirectory /var/lib/tor
HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80
```



KUVA 4:torrc-tiedosto

Tor on käynnistettävä uudestaan, jolloin asetukset tulevat voimaan. Käynnistyessään uudestaan Tor luo linkin, jota käytetään myöhemmin staattisen web-sivuston linkkinä Tor-verkossa. Tämä linkki on .onion päätteinen. Tor -ohjelmisto käynnistetään uudestaan komennolla:

```
sudo service tor restart
```

Tor-ohjelman luoma linkki on tallennettu */var/lib/tor/hidden_service/hostname* -tiedostoon, joka voidaan tarkistaa komennolla:

```
sudo cat /var/lib/tor/hidden_service/hostname
xlclklszcjk5ry5t.onion
```

Tämä on julkinen linkki, jota käytetään myöhemmin web-palvelimen asettamisessa toimintaan Tor-verkkoon. Tor loi myös yksityisen avaimen, joka on luettavissa */var/lib/tor/hidden_service/private_key* -tiedostossa. Tämä tiedosto on erittäin tärkeää pitää omassa tiedossa, sillä tiedostossa olevalla tiedolla voi kuka tahansa esittäytyä luotuna piilopalveluna.

4.4 Web-palvelin ja sen liittäminen Tor-verkkoon

Web-palvelimen asennuksen ja Tor-verkkoon liittämisessä käytetään seuraavaa järjestystä:

1. Ladataan ja asennetaan Nginx-web-palvelin
2. Luodaan web-sivusto
3. Liitetään web-sivusto Tor-verkkoon
4. Tarkistetaan, että sivusto on saavutettavissa Tor-verkosta

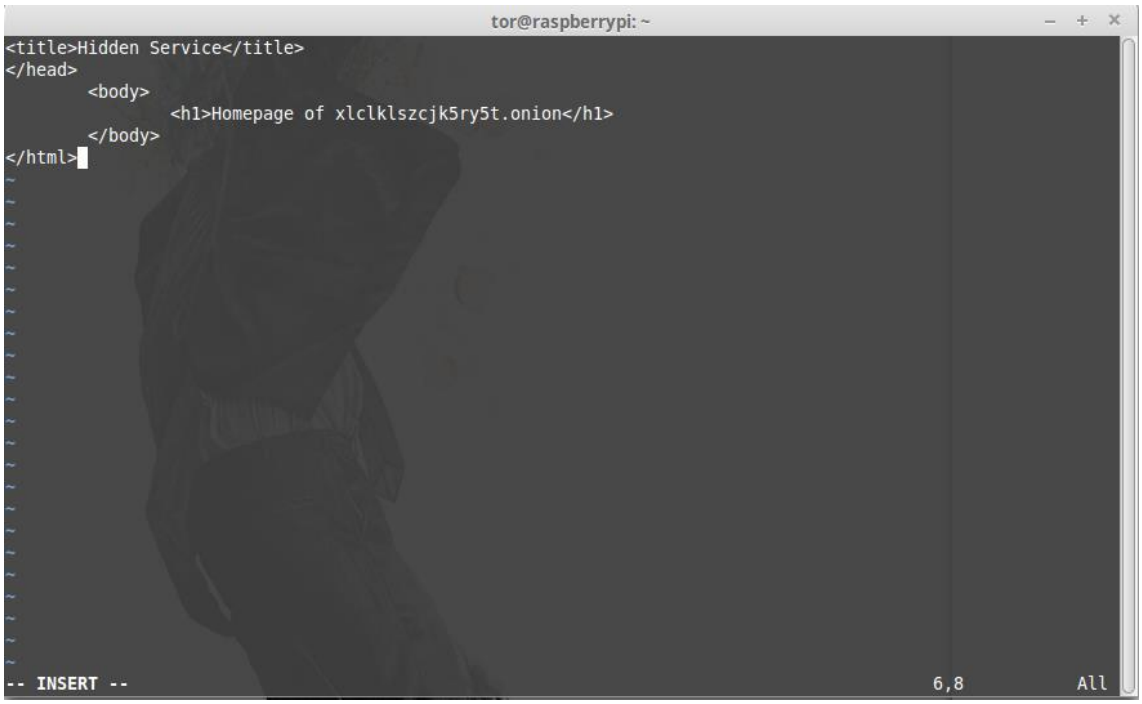
Nginx on web-palvelin, joka on keskittynyt suorituskykyyn ja vähäiseen muistin käyttöön. Nginx on Igor Sysoevin kehittämä sovellus. Se asennetaan kuin muutkin ohjelmat paketinhallinnasta. Komento on *sudo apt-get install nginx*. Komento lataa ja asentaa kaikki tarvittavat tiedostot ja ohjelmat. Nginxin asetustiedosto sijaitsee polussa /etc/nginx/nginx.conf

Luodaan kansio, jossa Tor-verkossa oleva web-sivu on ja annetaan sille Nginxin tarvitsemat pääsyoikeudet:

```
sudo mkdir -p /var/www/hidden_service/
sudo chown -R www-data:www-data /var/www/hidden_service/ && sudo chmod 755 /var/www
```

Juuri luotuun kansioon lisätään *index.html* tiedosto, joka tulee olemaan etusivuna Tor-verkossa. Tähän tiedostoon lisätään tiedot, joita halutaan web-sivustolla ylläpitää (kuva 5).

sudo vim /var/www/hidden_service/index.html



KUVA 5: index.html tiedoston sisältö

Tämän tiedoston lisäksi luodaan tiedosto, jotta Nginx osaa käyttää luotua sivustoa. Nämä tiedot lisätään tiedostoon */etc/nginx/sites-available/hidden_service*. Tässä tiedostossa on tiedot osoitteesta, jota web-palvelin kuuntelee, eli mistä on pääsy, missä sivuston tiedostot sijaitsevat ja mitä palvelinnimeä käytetään. Lisätyt tiedot ovat:

server {
listen 127.0.0.1:80;

root /var/www/hidden_service/;
index index.html;
server_name xlclklszcjk5ry5t.onion;
}

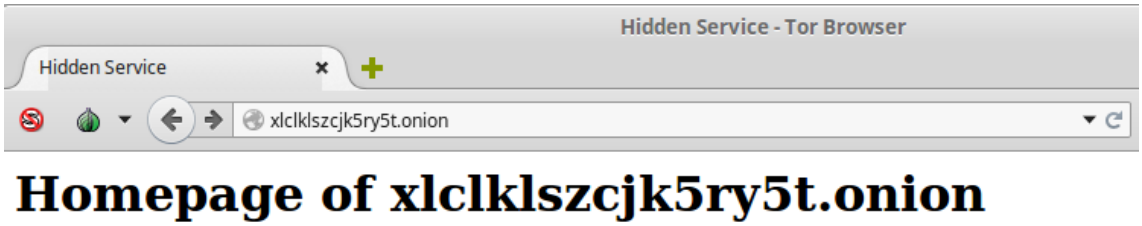
Nyt on asetettu tarvittavat tiedot Nginxin saataville, mutta laitetaan ne vielä julkisesti saataviksi. Se tehdään luomalla symbolinen linkki */etc/nginx/sites-available/hidden_service* ja */etc/nginx/sites-enabled/hidden_service* tiedostojen välille. Tämä symbolinen linkki toimii kuten pikakuvake. Komento symbolisen linkin luomiseksi on:

```
sudo ln -s /etc/nginx/sites-available/hidden_service /etc/nginx/sites-enabled/hidden_service
```

Kaikki tarvittavat tiedostot on luotu ja asetukset on tehty: web-sivusto on luotu ja asetettu Nginx:n käytettäväksi, sekä asetettu sivusto toimimaan Tor-verkossa. Jotta kaikki asetukset tulevat voimaan, pitää Nginx käynnistää uudestaan komennolla:

```
sudo service nginx restart
```

Nyt web-sivustoon pääsee käsiksi Tor-verkon kautta. Tarkistetaan, että kaikki toimivat selaamalla xlclklszcjk5ry5t.onion osoitetta Tor Browser -selaimella (kuva 6).



Kuva 6: Web-sivusto Tor-verkossa

4.5 Keskustelupalstan asennus, konfigurointi ja liittäminen Tor-verkkoon

Simple Machines Forum (lyhennettynä SMF) on avoimen lähdekoodin keskustelupalstaohjelmisto, jonka on kehittänyt Simple Machines. SMF käyttää hyödykseen PHP- ja MySQL-ohjelmistoja, jotka pitävät olla asennettuna ennen keskustelupalstan asennusta.

Keskustelupalstan asennus- ja asetusjärjestys on seuraava:

1. Asennetaan keskustelupalstan tarvitsemat ohjelmat: MySQL ja PHP
2. Luodaan MySQL-tietokanta
3. Ladataan keskustelupalstan ohjelmisto
4. Asennetaan keskustelupalstan ohjelmisto
5. Liitetään keskustelupalsta Tor-verkkoon
6. Tarkistetaan, että keskustelupalsta on saavutettavissa Tor-verkosta

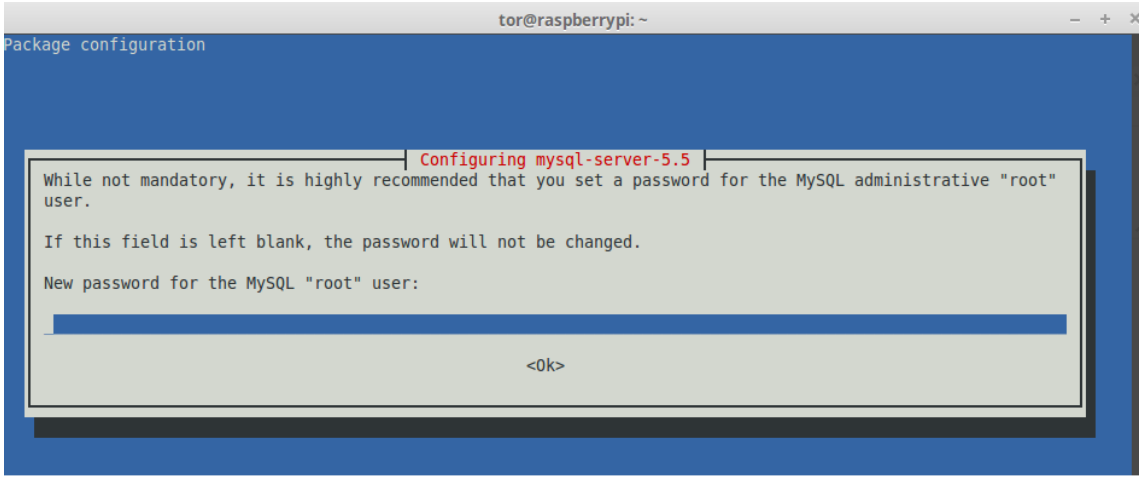
PHP on web-palvelinympäristössä käytetty ohjelmointikieli. SMF käyttää paljon hyödykseen PHP:tä. Se asennetaan komennolla:

sudo apt-get install php5-fpm php-apc

MySQL on tietokantaohjelmisto. Keskustelupalsta tallentaa MySQL- tietokantaan tietoja, joita keskustelupalsta käyttää hyödykseen. Tiedot, kuten käyttäjien käyttäjätunnukset, salasanat, kirjoitetut viestit ja niin edelleen sijaitsevat tässä tietokantaohjelmistossa. MySQL ja liitännäinen, joka sallii PHP:n käyttävän MySQL:ää, asennetaan komennolla:

sudo apt-get install mysql-server php5-mysql

Asennuksen jälkeen MySQL pyytää luomaan pääkäyttäjän salasanan (kuva 7). Salasana laitetaan kahdesti, jotta varmistetaan, että salasana on laitettu oikein.



KUVA 7: MySQL pääkäyttäjän salasana

Asennuksen jälkeen luodaan tietokanta, käyttäjä ja annetaan tälle käyttäjälle oikeudet tietokantaan. MySQL:ään kirjaudutaan komennolla:

```
mysql -u root -p
```

Luodaan tietokanta nimeltä *hiddenforum* ja tietokantakäyttäjä nimeltä *forumuser* ja annetaan käyttäjälle salasana *WuCLRnWsxeM2WpD*. Tällä käyttäjätunnuksella ja salasanalla yhdistetään SMF tietokantaan myöhemmässä vaiheessa.

```
CREATE SCHEMA hiddenforum;
CREATE USER 'forumuser'@'localhost' IDENTIFIED BY 'WuCLRnWsxeM2WpD';
GRANT ALL PRIVILEGES ON hiddenforum.* TO 'forumuser'@'localhost';
FLUSH PRIVILEGES;
QUIT;
```

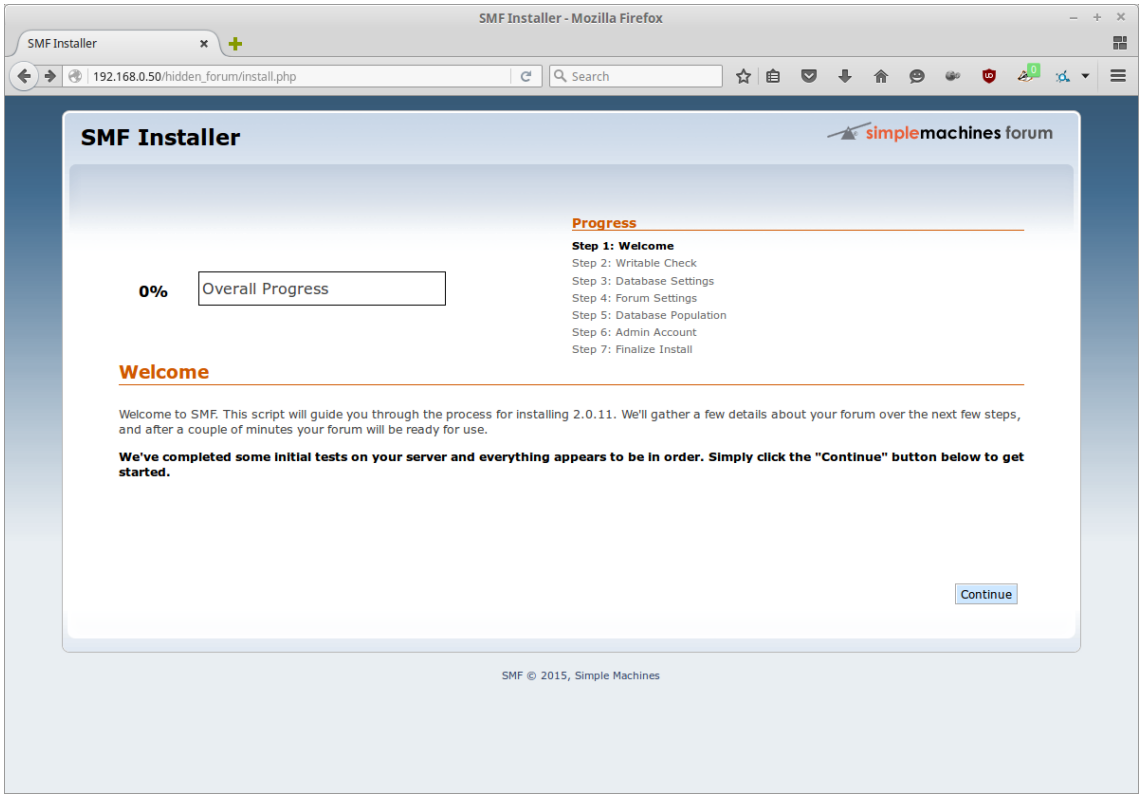
Simple Machines Forum -ohjelmisto ladataan sivuston lataussivulta. Ohjelma voidaan ladata suoraan palvelimelle *wget* komennolla. Lataushetkellä uusin versio on 2.0.11. Ohjelma ladataan */tmp/* -kansioon komennolla:

```
wget -P /tmp/ http://download.simplemachines.org/index.php/smf_2-0-11_install.tar.gz
```

Ohjelma on ladattu pakatussa muodossa, joka pitää purkaa, jotta ohjelma voidaan asentaa. Luodaan kansio */var/www/hidden_forum* ja puretaan ohjelma kyseiseen kansioon komennoilla:

```
sudo mkdir /var/www/hidden_forum
cd /var/www/hidden_forum/
sudo tar xfz /tmp/smf_2-0-11_install.tar.gz
```

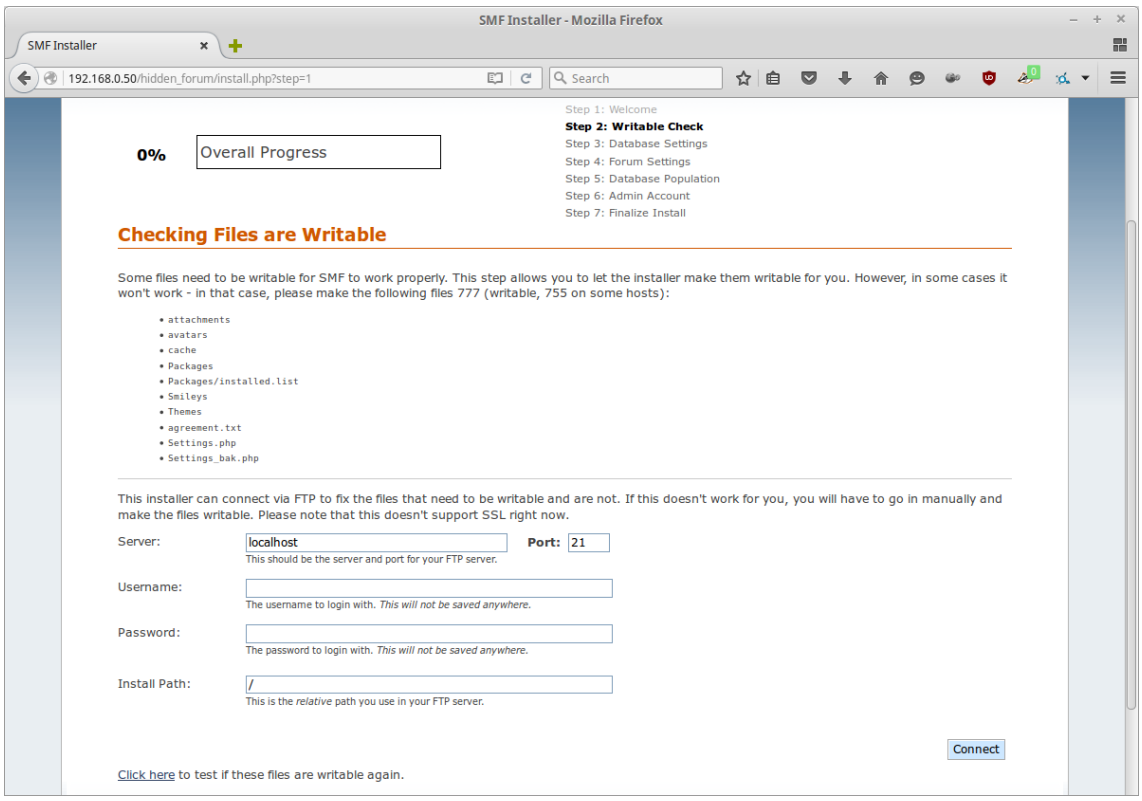
Tiedostot ovat paikallaan, joten voidaan aloittaa keskustelupastan asennus. Asennus tehdään selaimen avulla, joten selaimella avataan osoite http://192.168.0.50/hidden_forum/install.php (kuva 8).



KUVA 8: Simple Machines Forum asennussivu

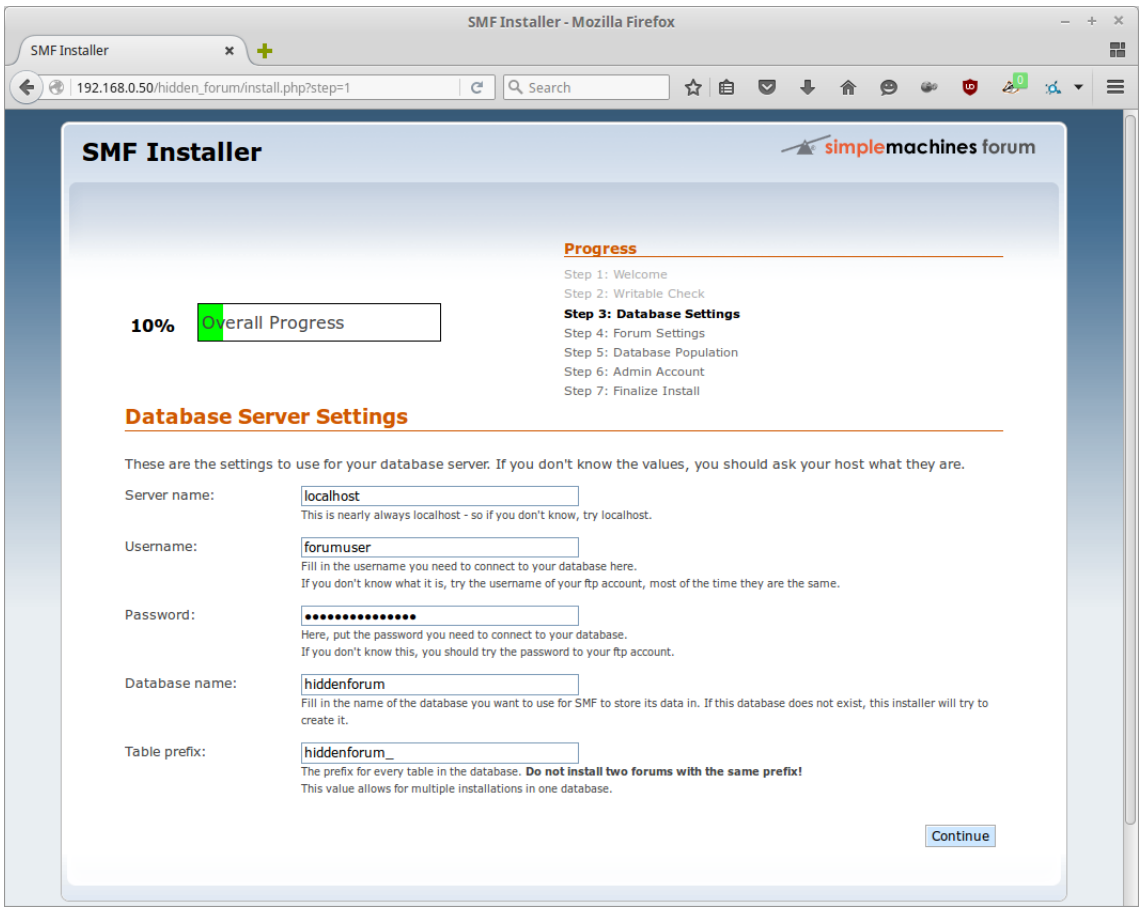
Jatketaan asennusta valitsemalla *Continue.* Asennus huomauttaa, että seuraaviin kansioihin kuuluu olla kirjoitusoikeudet (kuva 9). Oikeudet annetaan *chown* komennolla www-data käyttäjälle ja www-data käyttäjäryhmälle komennolla:

```
sudo chown -R www-data:www-data attachments avatars cache Packages Smileys Themes agreement.txt Settings.php Settings_bak.php
```



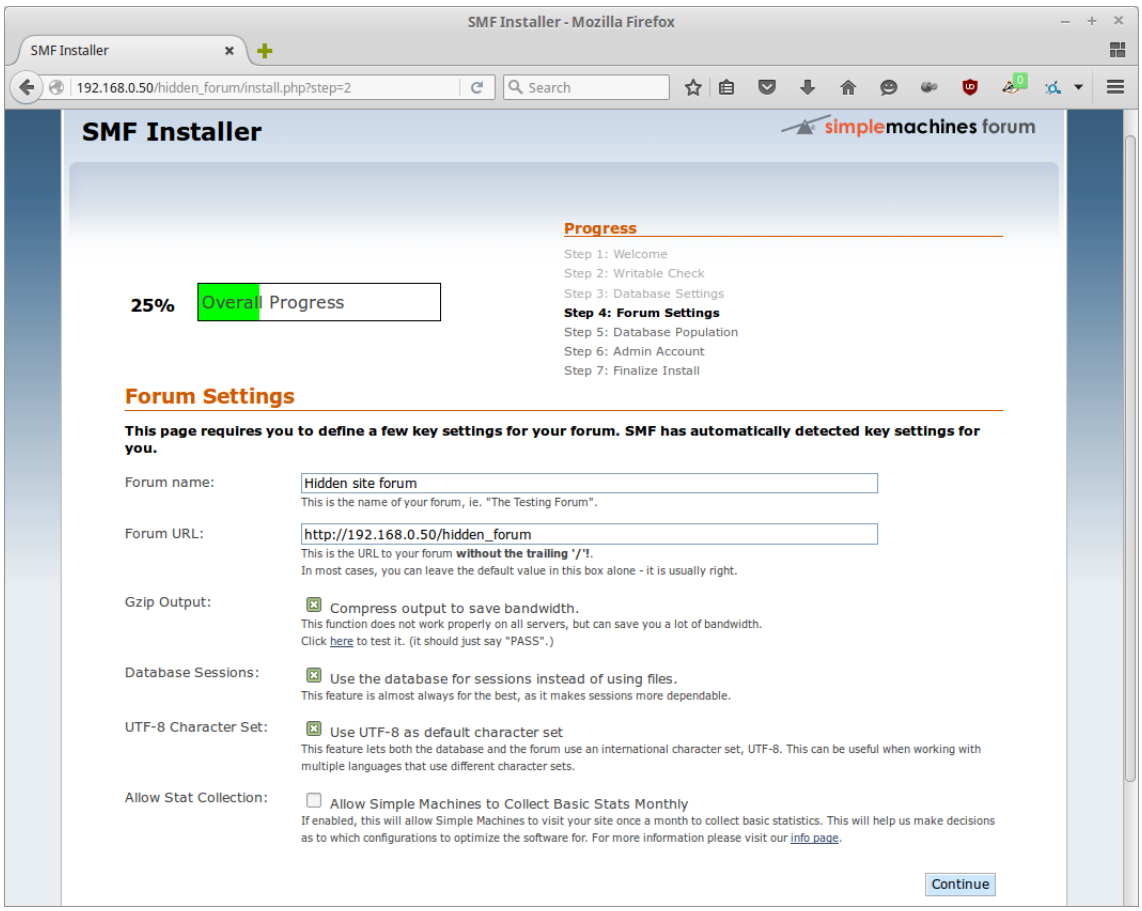
KUVA 9: Simple Machines Forum kansioiden ja tiedostojen kirjoitusoikeus tarkistus

Tarkistetaan, että tarvittavat oikeudet ovat oikein sivun alalaidassa olevasta linkistä. Sivu aukeaa uudelleen ja näyttää etenemisprosentiksi 10, jos oikeudet ovat kunnossa. Seuraavaksi laitetaan MySQL-palvelimen tiedot, jotka luotiin aiemmin. Käyttäjätunnus *forumuser*, salasana *WuCLRnWsxeM2WpD*, tietokanta *hiddenforum* (kuva 10).



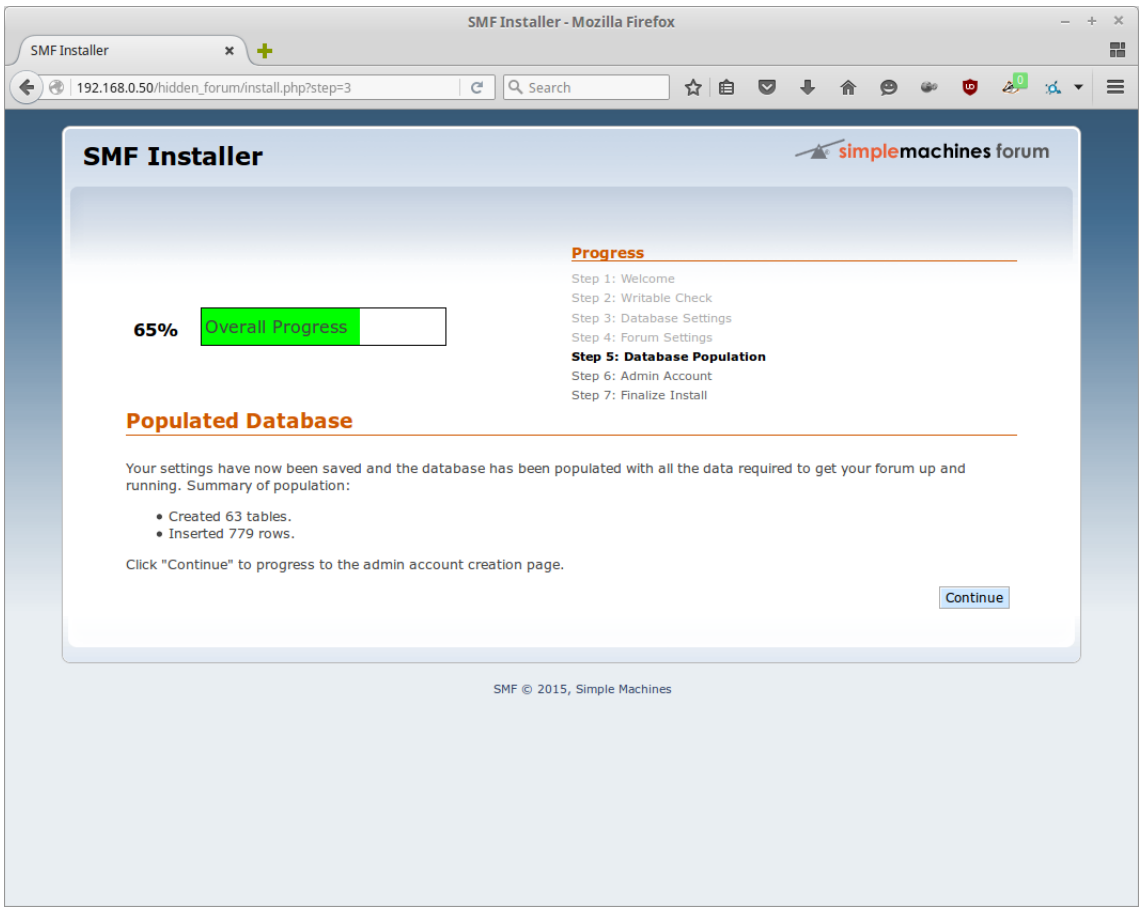
KUVA 10: Simple Machines Forum tietokantatietojen asennus

Keskustelupalstalle annetaan nimi *Hidden Site Forum* ja jätetään muut asetukset alkuperäisiksi (kuva 11).



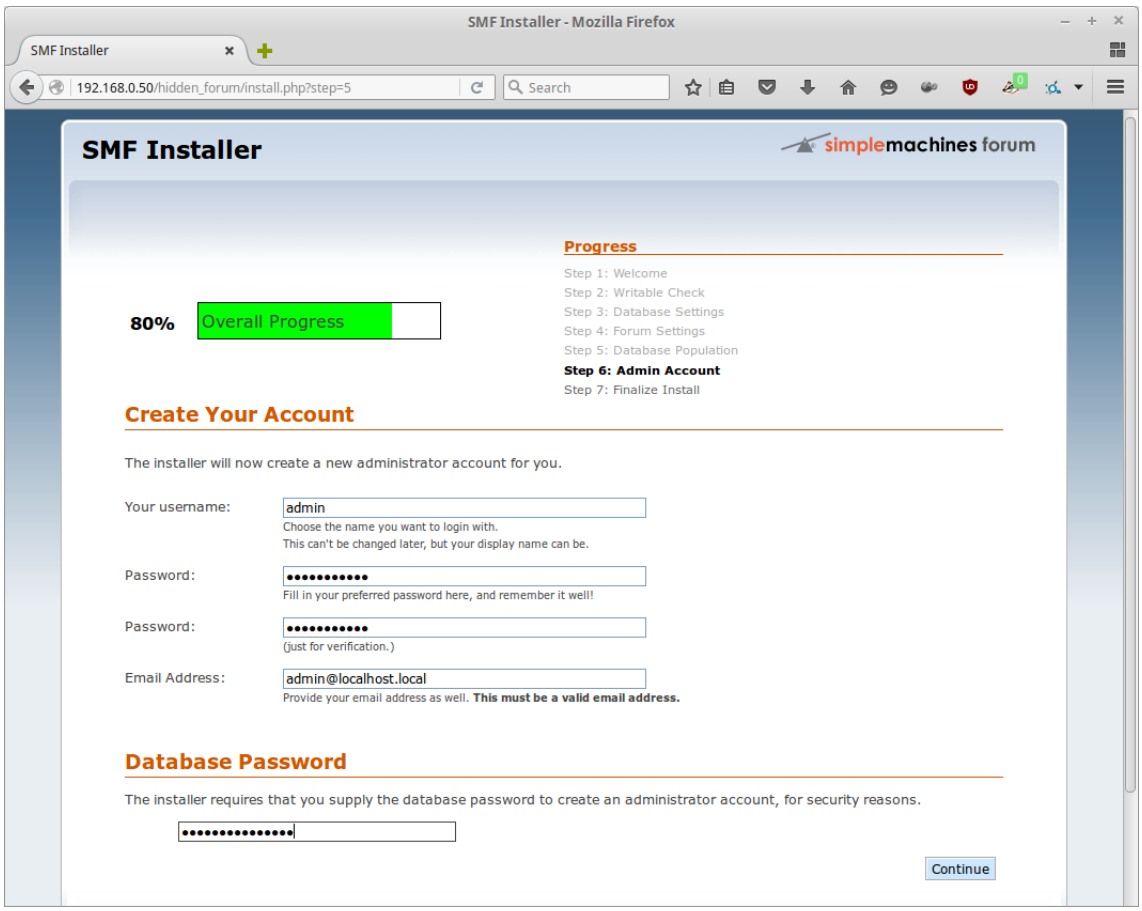
KUVA 11: Simple Machines Forum keskustelupalstan tiedot

Kun tiedot on tallennettu tietokantaan, valitaan *Continue* ja siirrytään keskustelupalstan pääkäyttäjätunnuksen lisäämiseen (kuva 12).



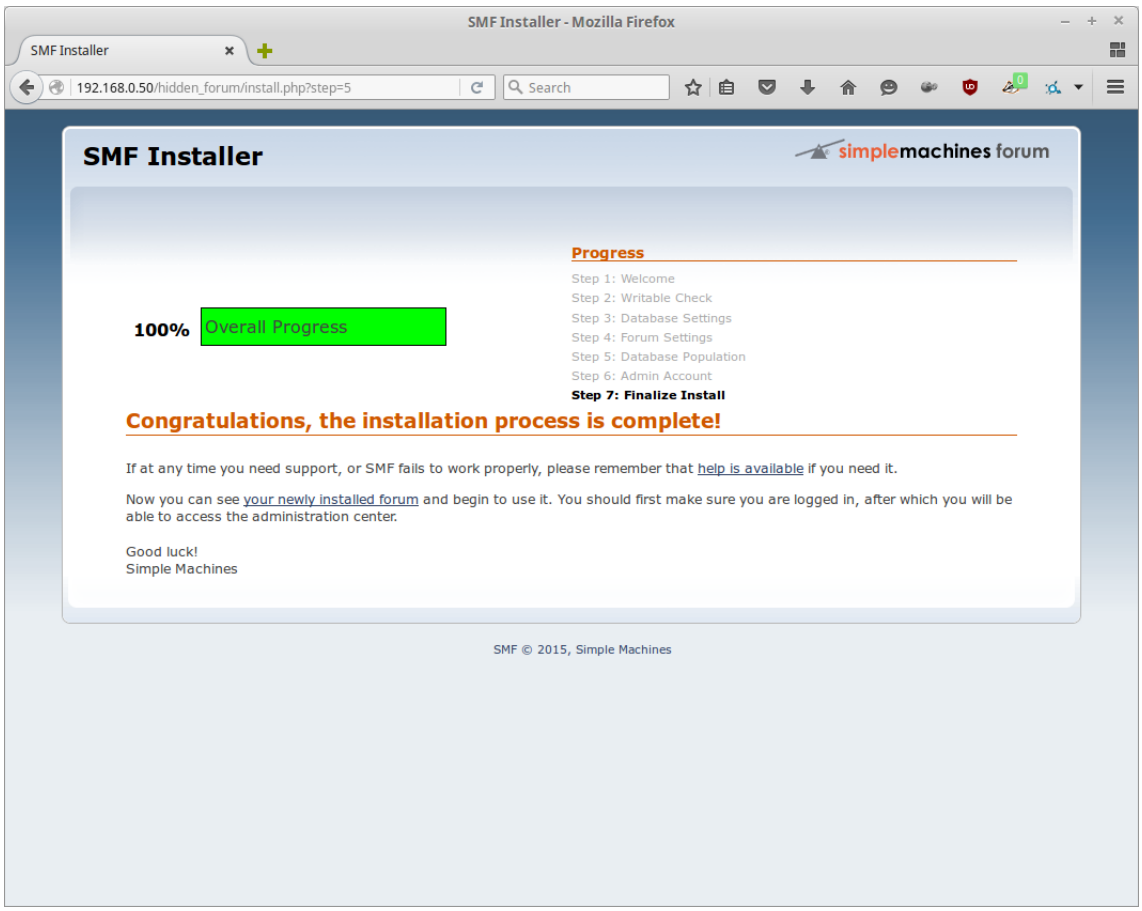
KUVA 12: Simple Machines Forum tietokantatietojen lisäys

Sivuston pääkäyttäjätunnukselle annetaan kirjautumisnimi ja salasana (kuva 13). Tällä tunnuksilla kirjaudutaan keskustelupalstalle ja sillä on keskustelupalstan pääkäyttäjäoikeudet. Vaikka asennus pyytää laittamaan toimivan sähköpostiosoitteen, ei sen tarvitse olla toimiva. Lisätään sähköpostiosoite, jolla voidaan varmistaa, että tietoa ei vahingossakaan lähetetä ulospäin, kuten admin@localhost.local. Samassa kohdassa annetaan myös tietokannan salasana, jotta tiedot voidaan kirjoittaa tietokantaan.



KUVA 13: Pääkäyttäjätunnuksen ja salasanan asettaminen

Keskustelupalstan asennus on valmis (kuva 14).

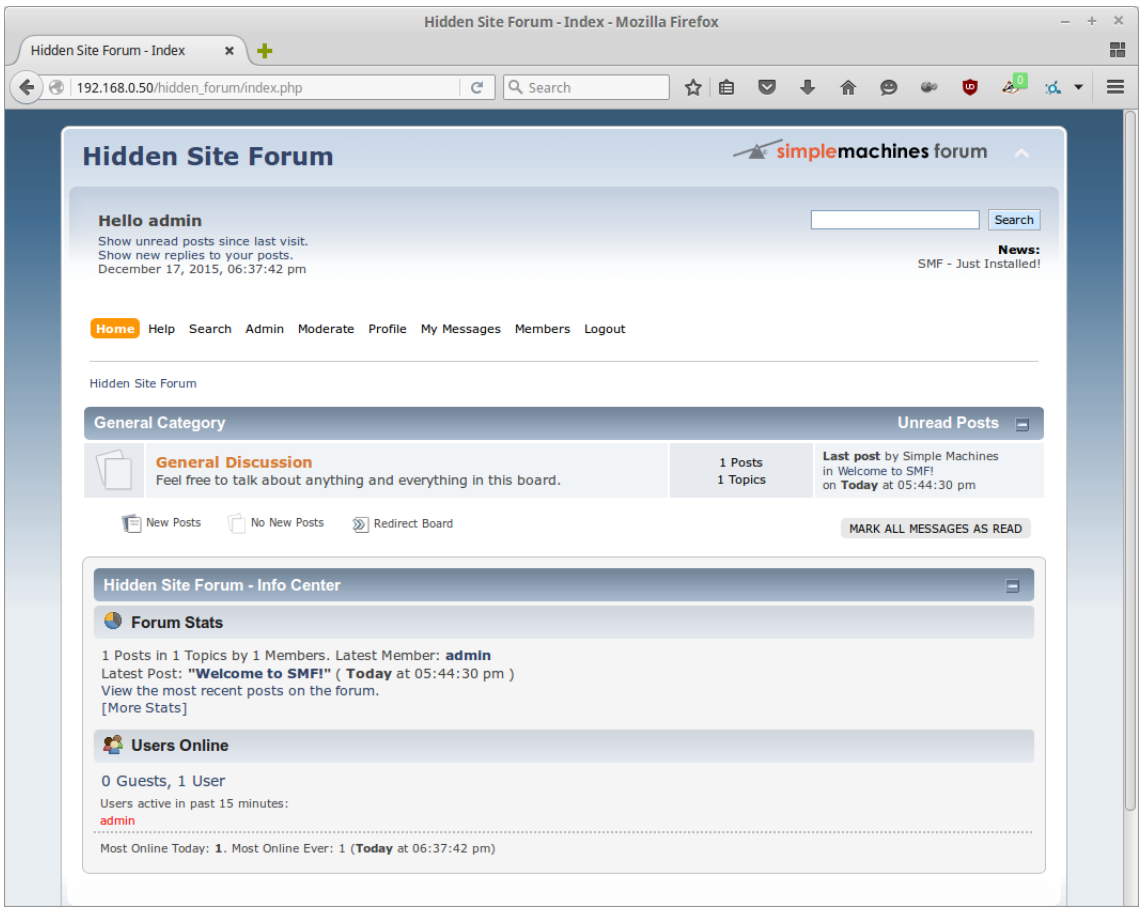


KUVA 14: Simple Machines Forum asennus on onnistunut

Jotta kukaan ei pääse käsiksi käytyyn asennusprosessiin, poistetaan palvelimelta *install.php* -tiedosto komennolla:

```
sudo rm /var/www/hidden_forum/install.php
```

Keskustelupalstalle pääsee nyt käsiksi lähiverkosta osoitteesta http://192.168.0.50/hidden_forum/index.php (kuva 15).



KUVA 15: Simple Machines Forum etusivu

Seuraavaksi palvelimen asetukset muokataan toimimaan Tor-verkossa. Lisätään */etc/tor/torrc* -tiedostoon tiedot, mitä palvelua ja porttia Tor kuuntelee. Samassa tiedostossa on tiedot aiemmin luodusta web-sivustosta.

HiddenServiceDir /var/lib/tor/hidden_forum/
HiddenServicePort 80 127.0.0.1:8080

Tor-ohjelma käynnistetään uudestaan, jolloin äsken asetetut tiedot tulevat voimaan. Samalla Tor-ohjelma luo tiedoston, josta voidaan tarkistaa, mitä .onion-osoitetta käytetään keskustelupalstan saavuttamiseen Tor-verkon kautta.

sudo service tor restart
sudo cat /var/lib/tor/hidden_forum/hostname
3x3pgkebmo6hdm32.onion

Tällä 3x3pgkebmo6hdm32.onion osoitteella konfiguroidaan keskustelupalstan saavuttaminen Tor-verkon kautta. Luodaan uusi tiedosto */etc/nginx/sites-available/hidden_forum*, jossa on tarvittavat tiedot Nginx -web-palvelimelle

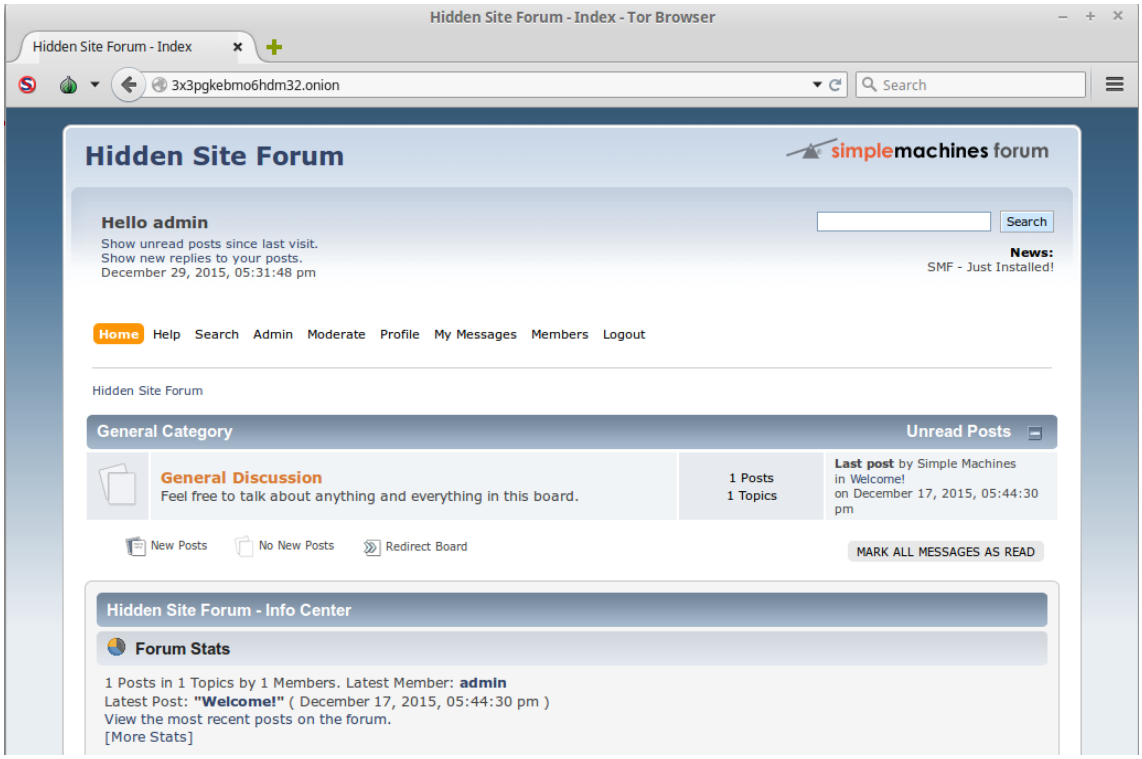
```
sudo vim /etc/nginx/sites-available/hidden_forum
```

```
server {
    listen 127.0.0.1:8080;
    server_name 3x3pgkebmo6hdm32.onion;

    root /var/www/hidden_forum/;
    index index.html index.htm index.php;

    location / {
        try_files $uri $uri/ /index.html;
        }

    location ~ \.php$ {
            try_files $uri =404;
            fastcgi_pass unix:/var/run/php5-fpm.sock;
            fastcgi_index index.php;
           fastcgi_param SCRIPT_FILENAME
          $document_root$fastcgi_script_name;
          include fastcgi_params;
        }
 }
```

Lisäksi muutetaan keskustelupalstan asennuksessa käytetty osoite käyttämään oman IP-osoitteen sijasta 3x3pgkebmo6hdm32.onion-osoitetta. Muokataan tiedoston */var/www/hidden_forum/Settings.php* kohtaan *$boardurl ='http://3x3pgkebmo6hdm32.onion';*. Nginx käynnistetään uudestaan, jolloin uudet asetukset tulevat voimaan.

```
sudo service nginx restart
```

Keskustelupalsta on saavutettavissa Tor-verkon kautta osoitteesta http://3x3pgkebmo6hdm32.onion (kuva 16).



KUVA 16: Keskustelupalsta Tor-verkossa

5 POHDINTA

Tässä opinnäytetyössä käytiin läpi, kuinka Tor-verkossa voidaan julkaista web-sivusto ja keskustelupalsta. Suurin osa tehtävästä työstä on samaa kuin muutenkin näiden palvelujen julkaiseminen, joten käytännössä Tor-verkkoon palveluiden lisääminen ei juurikaan työtä lisää. Tietoturva on vain vielä tärkeämmässä osassa, sillä oman henkilöllisyyden paljastavia tietoja, kuten IP-osoite, voi tapahtua vahingossa.

Kaksi palvelua julkaistiin osoitteissa http://xlclklszcjk5ry5t.onion ja http://3x3pgkebmo6hdm32.onion. http://xlclklszcjk5ry5t.onion on pelkistetty html-sivusto ja http://3x3pgkebmo6hdm32.onion on keskustelupalsta. Nämä palvelut ovat saavutettavissa vain Tor-verkon kautta.

Tietoturvan kannalta nämä palvelut ovat mahdollisesti haavoittuvaisia, sillä ohjelmat ladattiin paketinhallinnan kautta. Paketinhallinnassa ei täysin uusimpia ohjelmia ole saatavilla, joten joitain haavoituksia voi olla korjaamatta. Uusimmat versiot olisi tärkeintä olla ohjelmista web-palvelin Nginx sekä Tor. Nämä ovat ladattavissa ohjelmistokehittäjien omilta sivuilta, joskin asennus on hieman erilainen.

Tietoturvaa voisi lisätä myös käyttämällä eri laitteita Tor-verkkoon liittämisessä ja web-palvelimen hallinnassa. Tor-verkko ohjaisi ainoastaan web-palvelimelle kuuluvan liikenteen. Kun web-palvelimelta ei ole suoraa liikennettä internetiin, voidaan suojautua mahdollisilta haavoittuvaisuuksilta, jotka käyttäisivät muita palvelimen ohjelmia tai tietoja julkisen IP-osoitteen kaivamiseen. Opinnäytetyössä ei myöskään otettu huomioon mahdollista fyysistä pääsyä laitteistoon. Jos laitteistoon on fyysinen pääsy, ovat myös kaikki sivuston tiedot luettavissa. Tämän pystyisi estämään kryptaamalla kaikki palvelimen tiedot, jolloin laitteen käynnistyessä pääsy laitteelle avataan salasanalla.

Henkilö, joka osaa pystyttää palvelimen julkiseen verkkoon, osaa myös julkaista palvelimen Tor-verkossa. Tor-verkossa palveluiden julkaisemisessa on suurin osa samaa työtä kuin julkiseen verkkoon julkaistaessa. Tosin joitain asioita, kuten nimipalvelimen konfigurointia ei Tor-verkossa julkaistaessa tarvitse tehdä.

LÄHTEET

Schneier B. The Value of Privacy. Julkaistu 19.05.2006. Luettu 15.03.2016. https://www.schneier.com/blog/archives/2006/05/the_value_of_pr.html

Dingledine R., Mathewson N. & Syverson P. Tor: The Second-Generation Onion Router. Julkaistu 13.08.2004. Luettu 30.08.2015. https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf

Tor Network Status. Tarkistettu 30.01.2016. http://torstatus.blutmagie.de/

Finley K. Out in the Open: Inside the Operating System Edward Snowden Used to Evade the NSA. Julkaistu 14.04.2014. Luettu 08.03.2016. http://www.wired.com/2014/04/tails/

Electronic Frontier Foundation. What is Tor? Luettu 25.01.2016. https://www.eff.org/torchallenge/what-is-tor.html.

Wright J. How Tor Works? Julkaistu 28.02.2015. Luettu 05.02.2016. http://jordan-wright.com/blog/2015/02/28/how-tor-works-part-one/

The Tor Project. Bittorrent over Tor isn't a good idea. Julkaistu 30.04.2016. Luettu 05.02.2016. https://blog.torproject.org/blog/bittorrent-over-tor-isnt-good-idea

Goodin D., 25-GPU cluster cracks every standard Windows password in <6 hours. Julkaistu 10.12.2012. Luettu 21.03.2016. http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

Hanna B., How to setup a web server with Nginx/PHP on Raspberry Pi. Julkaistu 05.09.2013. Luettu 15.12.2015. http://workshop.botter.ventures/2013/09/05/how-to-setup-a-web-server-with-nginxphp-on-raspberry-pi/

Hanna B., How to setup a Simple Machines forum on Raspberry Pi. Julkaistu 10.09.2013. Luettu 15.12.2015. http://workshop.botter.ventures/2013/09/10/how-to-setup-a-simple-machines-forum-on-raspberry-pi/

Suomen Internetopas. Suojausmenetelmät. Luettu 24.03.2016. http://www.internetopas.com/yleistietoa/tietoturva/suojausmenetelmat/